UNIVERSIDADE ESTADUAL DA PARAÍBA

CENTRO DE CIÊNCIAS JURÍDICAS

CURSO DE DIREITO

SEGURANÇA DA INFORMAÇÃO CORPORATIVA

ASPECTOS E IMPLICAÇÕES JURÍDICAS

Aluno: Cláudio de Lucena Neto

Orientador: Antônio Silveira Neto

Campina Grande, fevereiro de 2003

Síntese

Na sociedade em que o bem mais valioso é o conhecimento humano, a discussão acerca da segurança da informação, ganha contornos de extrema relevância. A influência, o impacto e as soluções que o direito, em conjunto com outros campos inter-relacionados da atuação humana, busca para disciplinar as relações daí oriundas constituem o tema deste trabalho, que procura a definição dos conceitos, a compreensão dos mecanismos técnicos integrantes, e a análise comparativa de resultados e números que demonstram o alcance e a importância jurídica da matéria em comento.

Aborda-se o estudo de aspectos como o direito à privacidade, experiências de ataques e invasões a sistemas de informação, bem como de acidentes e circunstâncias que implicam em perda de dados. A isso, alia-se a observação dos instrumentos legais hoje disponíveis, concernentes à normatização de relações jurídicas empresariais envolvendo a Tecnologia e a Segurança da Informação.

Por fim, faz-se referência aos aspectos da responsabilidade civil decorrente destas relações, com a finalidade de estreitar a compreensão do fenômeno e de municiar as empresas e os profissionais a elas relacionados com um instrumento de apoio à avaliação de riscos com respeito à segurança da informação, e suas implicações e conseqüências jurídico-legais.

Sumário

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and except in darkness, every moment scrutinized.

George Orwell, 1984.

Apresentação

O desenvolvimento da sociedade contemporânea - a sociedade da informação -, na qual destaca-se como principal capital o conhecimento humano[1], traz consigo, tanto a necessidade de reavaliação de determinados conceitos e procedimentos técnicos, quanto de elaboração e definição de novos métodos e princípios que haverão de nortear e de buscar conferir equilíbrio às relações entre os indivíduos desta própria sociedade.

A informação, produto direito deste capital do conhecimento humano, é um dos bens de maior valia neste novo panorama mundial. Por esta razão, a sua guarda e a sua manutenção para uso eficiente e seguro deve ser objeto de preocupação de todos os segmentos da sociedade.

Com efeito, o tema já preocupa e ocupa diversas áreas da atuação humana, desde a Tecnologia da Informação, que procura desenvolver ferramentas, aplicativos e técnicas que venham a possibilitar o controle prático e efetivo desta segurança, passando pela Administração, que procura soluções para o gerenciamento das questões e dos recursos humanos envolvidos na manutenção da integridade de dados, chegando até o Direito, que, enquanto sistema normativo, tem como função precípua o estabelecimento de critérios que tornem a convivência social pacífica e equilibrada.

O impacto do problema no Direito é claro, à medida em que o uso indevido, inadequado e desautorizado da informação tende a causar significativos prejuízos, danos de naturezas e volumes os mais diversos, que, já começando a ser quantificados pelas empresas, reclamam reparação.

Dentro, ainda, do próprio Direito, é fácil constatar que o problema alcança vários de seus ramos. A segurança da informação suscita discussão em matéria de Direito Administrativo, vez que o Estado passa a valer-se de grandes bancos de dados públicos para tornar determinados serviços mais ágeis e acessíveis à população. O Direito Penal, por sua vez, não pode estar alheio à questão, dado que tem urgência em tipificar as

---

[1] LOBO, Paulo. *Di reito e Gbbalização*. FACTUM, Informativo Jurídico. Campina Grande, set.1998. p.02

condutas violadoras dos seus princípios, de forma a fazer com que aquelas que porventura mostrem-se mais danosas tenham punição mais gravosa. O escopo deste trabalho, porém, há de se restringir a uma análise do problema no plano cível, comercial, empresarial, sem descuidar de traçar, quando cabível, os devidos paralelos com os demais segmentos do direito.

Inobstante a escassa literatura técnico-científica acerca do tema, pesquisas e estatísticas têm sido feitas com surpreendente regularidade, o que demonstra a urgente necessidade da compreensão fática do fenômeno.

O sigilo, a privacidade e a certeza não são os únicos problemas trazidos pela necessidade de segurança da informação.

Recente pesquisa realizada pelo instituto *Forrester Research* dá conta de que *em 62% das empresas americanas os funcionários acessam* sites *de sexo e de bate-papo durante o expediente. Pelas contas do instituto, isso representa uma perda anual de 470 milhões de dólares em produtividade.*[2] Um outro estudo, desta vez do *SurfWatch*, revela que mais de 25% do tempo gasto pelos funcionários conectados à Internet não tem nenhuma relação com trabalho.[3] Perdas acidentais de dados, por sua vez, representam semelhante potencial de prejuízo, pelo que requerem igual tratamento de cautela.

São estas circunstâncias, que atentam diretamente contra a segurança da informação, e que, portanto, representam séria ameaça de dano e de prejuízo para as empresas, que serão objeto do estudo que segue, observadas sob a ótica da legislação, da doutrina jurídica e da tecnologia disponível.

---

[2] MILITELLO, Kátia. *Os perigos da Internet*. Infoexame, São Paulo, 2001. Disponível em: <http://www.infoexame.com.br>
[3] Ibid.

A Necessidade da Informação Segura

Um dos pontos determinantes na aceleração do desenvolvimento das relações de comércio, prestação de serviços, e das demais relações empresariais é o aspecto da segurança da informação que se troca ou armazena para posterior utilização.

O domínio da informação sempre teve fundamental importância para as corporações, sendo indispensável arma, do ponto de vista estratégico e empresarial. Dispor da informação correta, na hora adequada, significa ter um suporte imbatível para a tomada ágil e eficiente de decisão.

Obviamente, da forma como hoje é manipulada e armazenada, quando se faz extensivo uso dos meios e equipamentos eletrônicos, a informação passou a ser objeto de preocupação dos profissionais de Tecnologia da Informação, responsáveis pelos métodos de tratamento e pela sistematização dos dados, de modo a formar a referida base confiável para processos decisórios.

Contudo, dado o volume mundial de transações, sua expressividade no mundo de hoje, e o seu valor - patrimonial, inclusive –, o problema não pode deixar de importar ao Direito, mais uma vez chamado a intervir em nova manifestação de um fenômeno social, para regulamentá-lo.

A informação segura pressupõe requisitos[4] básicos,a saber:

- *autenticação* - a identidade de quem acessa os dados deve ser expressamente determinada;
- *confidencialidade* – proteção dos dados ou comunicações, através de técnicas específicas de segurança, contra acesso não autorizado;
- *autorização* - limitação ao uso dos dados disponíveis, a depender das permissões e dos poderes que deve ter cada usuário;

---

[4] COVALLA, Tom. *Safe and Sound*. Management Directions. IBM. EUA, set. 2001. n.21. p. 05.

- *privacidade na localização* - consistente na vedação de acesso indevido às áreas de localização (física) da informação.

Todos os requisitos acima, que são aplicáveis tanto à informação disponível na Internet quanto àquela restrita a uma máquina *standalone* ou a uma rede local, levam em consideração números, pesquisas e estatísticas obtidas por empresas especializadas em segurança, números estes que ajudam na adoção das contra-medidas cabíveis.

Recente pesquisa do *Computer Security Institute* garante que 75% dos servidores *Web* são vulneráveis à invasões. De acordo com Leonardo Scudere, *com toda esta mudança, muitos dos sistemas de segurança utilizados atualmente pelas empresas são pobres, trabalham de forma centralizada, estando preparados apenas para deter ameaças menores. Na Nova Economia, a segurança deve ser boa o suficiente para permitir o acesso de diferentes pontos, gerenciar todos os usuários cadastrados e usar software de detecção de intrusos*.[5]

E esse é, exatamente, um dos grandes desafios dos profissionais envolvidos com os problemas técnicos relativos à segurança da informação. É preciso buscá-la, mas sem ir de encontro à enorme tendência de flexibilização e de agilidade que vivem os mercados, de forma que as transações sejam realizadas da maneira mais conveniente – e segura – possível.

O Consultor Sidney Fabiani, diretor de Marketing da *Internet Security Systems* - *ISS*, lembra que apenas 5% das empresas utilizam softwares de detecção de intrusos. *Este tipo de software é o mínimo que uma empresa deve ter para evitar problemas de segurança.*[6]

Realmente, a grande causa dos problemas de segurança que hoje afligem as empresas é relativa ao acesso não autorizado da informação. No entanto, entre as ameaças mais freqüentes de falhas de segurança, estão aquelas que ocorrem pela porta da frente, isto é,

---

[5] TERZIAN, Françoise. *EUA vão perder US$ 10 bilhões Sistemas. B2B serão os mais afetados*, TCInet, 2001. Disponível em: <http://www.tcinet.com.br>

[6] Ibid.

o acesso ou o uso indevido por um funcionário da própria empresa, esteja ele insatisfeito ou mal-intencionado.

Responsáveis pelos Problemas de Segurança

	2000 %	2001 %
Hackers	25	43
Funcionários	33	31
Causa desconhecida	14	22
Fornecedores / Prestadores de Serviço	5	3
Concorrentes	2	1
Clientes	6	0
Outros	15	0

Fig. 01 - 7ª Pesquisa Nacional sobre Segurança da Informação
Fonte: Módulo Security Solutions –
e-security Magazine. julho de 2001

A 7ª Pesquisa Nacional sobre Segurança da Informação, realizada pela *Módulo Security Solutions*, divulgada no dia 30 de julho do corrente ano de 2001, após entrevistar 165 executivos de grandes empresas, tanto do setor público quanto do privado, nas mais variadas áreas de atuação, apontou o usuário interno como o mais propenso a causar problemas de segurança na empresa, seja em virtude de insatisfação, de vazamento de informação, de fraude, de espionagem ou até mesmo de sabotagem.

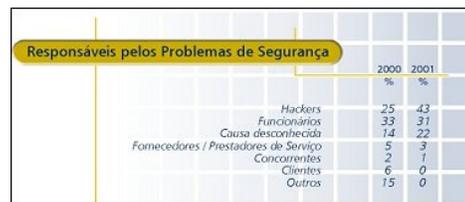
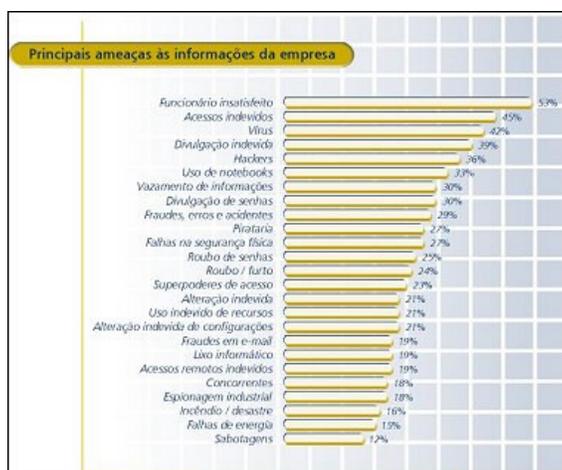



Fig. 02 - 7ª Pesquisa Nacional sobre Segurança da Informação
Fonte: Módulo Security Solutions – E-security Magazine.
julho de 2001

O mundo com Internet, ainda segundo Scudere, acaba por aumentar a insegurança das empresas. Os sistemas de hoje não são acessados somente pelos funcionários de uma empresa, mas também pelos fornecedores, clientes e parceiros. Os dados e aplicações não são mais centralizados. E o controle do sistema passa das mãos do gerente de informática (que até então decidia quem teria acesso a que) para a do homem de negócios (gerente de produto, comercial), que acaba por se preocupar mais com o faturamento do que com a segurança em si.

Até o fim do ano o crime eletrônico deverá causar um prejuízo de 10 bilhões de dólares aos Estados Unidos contra os 266 milhões de dólares de 1999, revela a já mencionada pesquisa do *Computer Security Institute*. As perdas ocasionadas pela falta de segurança nos sistemas das empresas envolvidas com o B2C (*business to consumer*) e o B2B (*business to business)* crescem na mesma proporção que a explosão da Internet.

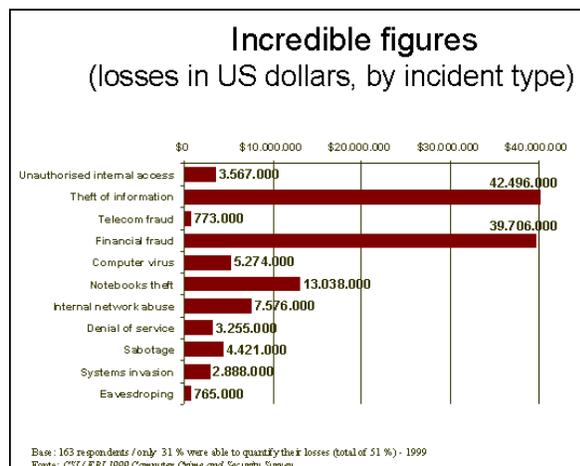
Números da Pesquisa de Segurança da Revista *Information Week* também revelam somas alarmantes referentes às perdas financeiras decorrentes de falhas na segurança de informação nas empresas.[7]

Por esta razão, estudo da *McKinsey*[8], indica que os *e-business* ligados a empresas de tijolo e cimento têm duas vezes mais chance de serem lucrativos do que as *start-ups* puras, pois se beneficiam da marca e do marketing de suas congêneres, o que acaba por associá-las a uma idéia de maior confiabilidade, cativando clientes mais conservadores.

Ainda de acordo com a pesquisa da Módulo, a contaminação por vírus e os ataques de *hackers* representam parcela significativa das ameaças à segurança nas corporações. O Brasil deve tomar especial cuidado com os números. Dos dez grupos de *hackers* mais ativos no mundo, cinco são brasileiros. Até o dia 22 de agosto de 2001, eles haviam invadido cerca de 3.000 *sites*.[9]

Classificação da Informação

O estado-da-arte da tecnologia permite que se estabeleçam estágios de proteção diferentes para categorias de informação que requeiram maior ou menor nível de segurança. Com efeito, nem toda a sorte de informação é crucial ou essencial a ponto de merecer cuidados manifestamente especiais. Por outro lado, determinada informação pode ser tão vital que o custo de sua integridade, qualquer que seja, ainda será menor que o custo de não dispor dela adequadamente.

---

[7] INFORMATION WEEK, PriceWaterhouseCoopers & Global Information Security Survey. Information Week. EUA, 2001.
[8] MILITELLO, Kátia. *Os perigos da Internet*. Infoexame, São Paulo, 2001. Disponível em: <http://www.infoexame.com.br>
[9] ZAKABI, Rosana. *HACKERS Os nossos são campeões*. Revista VEJA. São Paulo. set. de 2001. p. 76.

Dimitri Abreu[10], e Sean Boran[11] expõem, de forma bastante clara, a necessidade de classificação da informação em níveis de prioridade, obviamente, conforme a necessidade de cada empresa, bem como conforme a vitalidade daquela classe de informação para a manutenção das atividades da empresa:

- *pública* – informação que pode vir a público sem maiores conseqüências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;
- *interna* – o acesso a esse tipo de informação deve ser evitado, embora as conseqüências do uso desautorizado não sejam por demais sérias. Sua integridade é importante, porquanto não seja vital;
- *confidencial* – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;
- *secreta* – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia.

De forma que, tanto os cuidados, quanto a responsabilidade e o grau de envolvimento do pessoal eventualmente envolvido com a produção, guarda, manutenção e manipulação da informação devem obedecer a determinados critérios de classificação da importância e do nível de dependência da empresa com relação à referida informação.

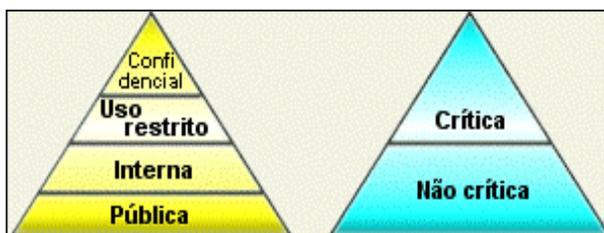



Fig 04. Esquema de classificação da informação segundo a importância de conteúdo e a necessidade de integridade

[10] ABREU, Dimitri. *Melhores Práticas para Classificar as Informações*. Módulo e-Security Magazine. São Paulo. ago. 2001. Disponível em: <http://www.modulo.com.br>
[11] BORAN, Sean. The IT Security Cookbook Information classification. EUA. dez. 1996. p. 16.

Privacidade - *The right to be left alone*

The right to be left alone – the most comprehensive of rights
and the right most valued by a free people.
Juiz Louis Brandeis, Olmstead v. U.S. (1928)

Obviamente, sempre que se fala em acesso à informação, deve-se lembrar que, em um estado democrático de direito, a intimidade e a vida privada são garantias constitucionais, e a mera ameaça a qualquer desses direitos é causa de grande comoção e movimentação social. A Constituição Federal, em seu art. 5º, incisos X e XII, dispõe, *verbis:*

> *X - ... são invioláveis a intimidade, a vida privada, a honra e a intimidade das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua utilização.*

> *XII - ... é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investiga;cão criminal ou instrução processual penal.*

Assim sendo, é de se esperar que o respeito à privacidade seja uma das grandes preocupações no tratamento seguro da informação. Por outro lado, a discussão a esse respeito é delicadíssima, visto que a autenticação, a identificação, conforme já exposto, são requisitos essenciais para que o acesso adequado à informação armazenada em meios eletrônicos possa ser devidamente controlado.

A questão é complexa, e de sua discussão se ocupam renomados autores, evidentemente preocupados com o inegável direito do cidadão à preservação de seus direitos, mas igualmente cônscios de que a proteção à integridade dos dados constitui uma garantia para este mesmo cidadão. Neste sentido, o eminente constitucionalista José Afonso da Silva comenta, com propriedade:

> *O perigo é tão maior quanto mais a utilização da informática facilita a interconexão de fichários com a possibilidade de formar grandes bancos de dados que*

> *desvendem a vida dos indivíduos, sem sua autorização e até sem seu conhecimento*[12]

Ora, é virtualmente impossível ao cidadão comum, ainda que lhe seja dado o direito de controlar a disponibilidade de suas informações pessoais nesses gigantescos e infindáveis bancos de dados, exercer, de fato, este direito. Se a parcela da vida humana que é monitorada, observada pelos outros no contexto dia-a-dia, ainda que volátil e temporária, já é suficientemente exposta a público, o que dizer da parcela de vida que é pesquisável, infinitamente menos transitória, que deixa rastros e registros escritos, visíveis e indeléveis?[13]

Cada dia mais os serviços de *e-government* ganham espaço, deixando as funções do estado mais acessíveis e as suas atitudes e políticas mais transparentes, o que parece ser muito positivo. Contudo, para que isso possa ser operacionalizado, enormes bases de dados públicas têm que ser criadas e disponibilizadas para acesso remoto. Sem uma política consistente de segurança, será informação privada – toneladas dela – exposta a quem quer que tenha acesso a um computador e um canal de acesso à rede, o que, admita-se, pode vir a ter conseqüências desastrosas.[14]

Caminhando na busca de uma solução compatível com os princípios de democracia e, ao mesmo tempo, que permita o necessário controle da informação, diversos estados e organismos internacionais já iniciaram o indispensável trabalho legislativo exigido.

França e Alemanha, esta última tendo sido uma das primeiras nações a regulamentar a matéria, têm codificações legais explícitas dispondo sobre a proteção da privacidade. A União Européia também dispõe de dispositivos normativos disciplinando o acesso, a coleta e o uso de informações privadas.

No Brasil, embora as implicações civis do uso indevido de dados privados já possam obedecer à legislação vigente, no que assim couber, com base no princípio da aplicação analógica da lei, o projeto de Lei n.º 234 tramita no Congresso Nacional, dispondo,

---

[12] SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 15. edição. Malheiros Editora. São Paulo. 1998. p. 213.
[13] LESSIG, Lawrence. The Architecture of Privacy. Conferência na Taiwan Net. Taipei. mar.1998. p. 02.
[14] PERDONCINI, Priscila. *Arquivos Públicos na Internet Ameaçam Privacidade*. InfoGuerra. ago. 2001. Disponível em: <http://www.infoguerra.com.br>.

especificamente, sobre os crimes contra a inviolabilidade de dados e de comunicações através de computadores, o que poderá contribuir para uma punição mais adequada pra aqueles que violam os princípios da privacidade em bases de dados.

Função Social da Privacidade

Com o enorme potencial de exposição de informação privada que a sociedade da informação oferece, é claro que o direito à privacidade vem assumindo papel relevante como escudo do cidadão contra o poder onipresente do *Big Brother* de ORWELL (1949).

Há razões, contudo, de inegável interesse público, que parecem justificar a necessidade de um mínimo de controle legal sobre o tráfego de informação, muito embora esteja claro que o direito à privacidade não deve ser confundido com o direito ao sigilo profissional, bancário, postal dentre outros já extensivamente disciplinados em textos legais vigentes.[15]

Da mesma forma que ocorreu ao longo dos séculos com o direito à propriedade, que, em seus primórdios, não conhecia limites[16], a privacidade absoluta pode desvirtuar-se, fazendo com que o indivíduo venha a tirar proveito de uma situação de anonimato – que também encontra vedação constitucional – passando a ser utilizada de forma nociva à sociedade que busca proteger.

Indicando que a esta é uma tendência bastante razoável, a Comissão de Educação do Senado aprovou, recentemente, projeto de lei que dispõe sobre as informações relativas ao acesso à Internet. Pela proposta, os provedores da Internet estarão obrigados a manter registros, por período não inferior a um ano, de todas as conexões realizadas por seus usuários. *Os registros das conexões entre provedores terão que indicar a data, o horário de conexão e desconexão, além do endereço eletrônico atribuído ao cliente*.[17]

---

[15] ALMEIDA, Gilberto Martins de. *As Empresas podem "grampear" o e-mail de seus funcionários?* Módulo e-Security News. Rio de Janeiro. 1999. Disponível em: <http://www.modulo.com.br>.
[16] VENOSA, Sílvio de Salvo. *Direito Civil*. Direitos Reais. Atlas. São Paulo. 2001. v. 04. p. 140.
[17] BRASIL EM TEMPO REAL. *Senado Aprova Normas de Acesso à Internet*. Brasília. ago. 2001. Disponível em: <http://www.emtemporeal.com.br>.

Por fim, vale a pena transcrever trecho no qual a Professora Lílian Minardi Paesani parece sintetizar de forma especialmente clara, *o que* e *como* devem ser consideradas as limitações ao indiscutível direito constitucional à privacidade, limitações essas que devem encontrar justificativas na prevalência do interesse coletivo, a partir da compreensão da *função social da privacidade*:

> *... podem ser impostos limites à normal esfera de privacidade* até contra a vontade do indivíduo*, mas em correspondência à sua posição na sociedade, se for de relevância pública. Nesses casos, será possível individualizar, se há interesse público em divulgar aspectos da vida privada do indivíduo. O interesse será relevante somente com relação à notícia cujo conhecimento demonstre utilidade para obter elementos de avaliação sobre a pessoa como personalidade pública, limitando, desta forma* – e não eliminando – *a esfera privada do próprio sujeito.*[18] (grifos da autora)

Ameaças Potenciais à Segurança da Informação

A compreensão das técnicas e dos métodos utilizados para burlar a segurança de sistemas de informação é de fundamental importância para a adoção das contra-medidas necessárias, bem como para possibilitar ao direito a definição de leis e normas genéricas e abstratas, objetivamente aplicáveis a esta natureza de relação jurídica.

Ataques

A *Amazon Books* garante que até hoje, nenhum dos seus mais de 2 milhões de consumidores em todo o mundo registrou uma única reclamação de uso indevido de cartão de crédito.[19] Infelizmente, esta não é a realidade de grande parte das empresas de informática existentes.

A invasão, tentada ou consumada, de bases de dados, a alteração ou paralisação de *websites*, de serviços e de sistemas de informação vem sendo uma constante no mundo da computação corporativa. Aproveitando-se das falhas de segurança das empresas, de

[18] PAESANI, Lilian Minardi. *Direito e Internet*; Liberdade de Informação, Privacidade e Responsabilidade Civil. Atlas. São Paulo. 2000. p. 48.

suas estruturas de rede ou de seus aplicativos, os ataques podem resultar em destruição, perda ou roubo de informação, infecção por código maligno (vírus, cavalos de Tróia, *worms*, etc.) ou simplesmente em acesso indevido, na visualização não autorizada, de determinada informação.

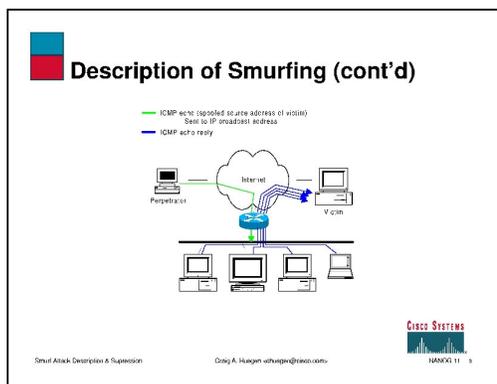
Eventualmente, se a responsabilidade pelo dano patrimonial efetivamente causado durante o ataque puder ser atribuída a alguém, o pedido de ressarcimento ainda seria cabível. Para a invasão, *strictu sensu*, sem perda, furto ou destruição comprovada de informação – o que muitas vezes acontece sem que a empresa sequer tome conhecimento – é impossível, pela legislação brasileira em vigor, qualquer tentativa de configuração de prejuízo reparável.

DoS (Denial of Service)

Muitas vezes ocorre de haver paralisação no funcionamento de um servidor, não em virtude de invasão direta, sem autorização, sem quebra de senha ou introdução de código maligno, mas através da ativação de muito mais tarefas do que a capacidade de processamento de qualquer máquina poderia suportar. São as chamadas técnicas de DoS - *Denial of Service* (negação de serviço). Quando um servidor "se nega" a continuar a operar normalmente, há excesso de solicitações de serviços, causando a paralisação.[20]

Muitas vezes, o acesso não autorizado já ocorreu, quando diversas outras máquinas foram infectadas com código especificamente preparado para o ataque. À chegada de uma condição, que pode ser um dia, um comando, uma mensagem, o ataque é disparado.

---

[19] REVISTA DA CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. *Com um pé no Futuro*. Brasília n.311. fev. 1999. p. 25
[20] PEREIRA, Cristiane Santos. Implementação de Políticas e Procedimentos de Segurança em Ambientes Internet. Universidade de Brasília. 2000. p. 19.

Diversas variações podem ser verificadas nesta modalidade de ataque, como a *Mail Bomb*, usada especificamente para inundar servidores de e-mail, ou *Smurfing*, procedimento que consiste em abarrotar um servidor de comandos *ping*[21], causando o mesmo efeito.

Mais uma vez, o eventual prejuízo advindo só poderá ser demandado em juízo caso comprovado o dano efetivo, diretamente decorrente da agressão perpetrada.

Armazenamento, Restauração e Integridade

A integridade dos dados é um outro aspecto de extrema relevância para quem é responsável pela segurança de informações. A perda da informação pode, por vezes, significar prejuízo incalculável, maior até mesmo do que o acarretado pelo uso desautorizado.

Isto porque, a utilização indevida da informação causa, pelo menos à primeira análise, meramente um abalo moral, que, neste momento, não é mensurável, exceto através das devidas estimativas que possam se seguir. As tarefas não são interrompidas, os serviços não sofrem descontinuidade.

A perda, seja ela total ou parcial dos dados, por seu turno, origina dano patrimonial direto. Embora o valor pecuniário das bases de dados, em princípio, também não seja determinado, há custos intrínsecos à administração dos dados que terão de ser despendidos uma vez mais, a exemplo da redigitação da informação, quando esta é possível, da nova coleta de dados, do reprocessamento, da reinstalação e da reconfiguração de sistemas, tarefas que oneram diretamente o orçamento daquele que é prejudicado por esta circunstância - para mencionar apenas as situações recuperáveis.

---

[21] comando de teste utilizado para detectar a acessibilidade de determinado endereço IP.

Além do mais, da mesma forma que as pessoas devem ter a sua privacidade respeitada, podendo exercer o direito de impedir o acesso indevido às suas informações de caráter pessoal, devem, também, dispor de acesso aos seus próprios dados, onde quer que estejam, assistindo-lhes o direito de consultá-los e de alterá-los, quando não corresponderem à verdade.

O IDC estima que o investimento das empresas em tecnologias que as auxiliem a contornar os problemas de armazenamento e restauração, bem como as ameaças de perda de dados chegue, em 2004, a 10,4 bilhões de dólares, investimento esse que já foi da ordem de 5 bilhões de dólares, há dois anos.[22]

Arquivos, discos, e mídias eletrônicas em geral são corrompidas pelas mais diversas razões: quedas ou elevações súbitas na tensão elétrica, falha de *hardware*, falha ou despreparo do *humanware,* dentre outras.

Normalmente, devem responder pela perda total ou parcial dos arquivos os profissionais responsáveis pela manutenção de sua integridade, ressalvados, obviamente, os casos onde a responsabilidade civil não lhes puder ser atribuída, conforme se verá mais adiante.

Por fim, é preciso que se ressalte que sobre o *backup*, espelho fiel dos dados, incidem todos os direitos à privacidade já discutidos e expostos, sendo terminantemente vedada, à luz dos ordenamentos jurídicos em vigor em grande parte das nações, o seu uso sem prévia e expressa autorização.

Acidentes

Por fim, não se pode deixar de considerar as possibilidades de prejuízos e de danos advindos de acidentes naturais e de situações oriundas de desequilíbrio ambiental.

Incêndios, alagamentos, explosões, desabamentos, terremotos, umidade radiação, poeira, ruído, superaquecimento, magnetismo, falhas de energia elétrica ou de sistemas

---

[22] BOTONI, Fernanda. *Sos Backup.* Infoexame, Rio de Janeiro. set. 2001. p. 110.

de comunicação, dentre diversas outras situações que, muitas vezes, estão fora do escopo de alcance das previsões razoáveis, podem ser responsáveis pela perda total, parcial, ou pela inconsistência das informações, causando dano, à primeira vista, indenizável.

Aspectos da Responsabilidade Civil pela Guarda da Informação

Não é pelo fato de estarem relacionadas ao ambiente dito virtual, que a segurança, a guarda, o uso e a manutenção da informação são obrigações de menor poder coercitivo, na forma da lei Ao contrário, estão sujeitas, inclusive, às sanções cabíveis, caso haja descumprimento. Muito embora o tema reclame e justifique exaustivo trabalho específico, não se pode deixar de traçar algumas considerações fundamentais.

Como já dito, alguns países já decidiram definir tipos penais a partir dos quais pretendem punir as práticas infracionais consideradas mais danosas. O Brasil ainda não dispõe de tal texto legal. O crime aqui praticado só poderá encontrar óbice e sanção jurídica se já estiver definido como tipo penal, sendo a tecnologia apenas o meio mediato – e ainda assim se o tipo não previr, expressamente, um outro meio – utilizado para a consecução do resultado.

Ainda assim, a responsabilidade civil pelo fato ou pelo dano causado à informação é imputável ao causador do resultado maligno, em virtude da possibilidade da aplicação analógica da lei cível, desde que obedeça aos pressupostos caracterizadores já familiares ao instituto: uma *ação*, ou uma *omissão*, que, mediante um *liame ou nexo de causalidade,* importe em um *resultado danoso*, mediante *culpa* do agente.[23]

Todas as relações jurídicas, e, por conseqüência, todos os agentes envolvidos e relacionados à guarda e à manipulação da informação estão sujeitos a responder civilmente por suas ações ou omissões. O incipiente estado de definições técnico-jurídicas, no entanto, restringe sensivelmente a chegada da tal matéria às cortes do país,

---

[23] STOCCO, Rui. *Responsabilidade Civil e sua Interpretação Jurisprudencial*. Revista dos Tribunais. São Paulo. 2000. p. 66.

à exceção de alguns poucos *leading cases*, que começam a escrever a história jurisprudencial da matéria.

Os ataques e invasões a sistemas de informação, segundo observação anterior, são passíveis de responsabilização no plano cível, à medida em que causem dano efetivo, assegurada a reparação do dano moral, e desde que o invasor ou agressor possa ser individualizado. Ora, não é necessário muita reflexão para entender que, com a garantia do direito à privacidade, aliada às limitações técnicas existentes, o rastreamento efetivo do responsável por um ataque é tarefa extremamente árdua, embora não impossível. Técnicas de *tracking* estão sendo desenvolvidas e grupos especiais do órgão competente, neste caso, a polícia, estão sendo treinados para lidar com a nova realidade que se lhes apresenta. Divisões de Alta Tecnologia já são uma realidade em muitas forças policiais no país e no exterior.

Em relação a serviços prestados pelas empresas, a responsabilização civil é tarefa menos abstrata. Isto porque os sujeitos da relação estão claramente definidos, dependendo o surgimento da obrigação de composição do dano apenas da prova do resultado daninho, do nexo de causa e da culpa.

Provedores de acesso, são agentes diretamente expostos a estas questões. Na maior parte das situações, suas ações estão relacionadas à aplicação da *teoria da culpa*, sendo essencial que se demonstre, efetivamente, a existência de imprudência, negligência ou imperícia para a responsabilização civil.[24]

Quanto à divulgação de conteúdo, cabe deliberar a respeito da responsabilidade civil do provedor de acesso. A ser obedecido o direito estrito à privacidade, nenhuma atitude pode tomar o provedor com relação à informação que trafega pelo seu domínio, quando for apenas o intermediário, o meio técnico. Assim sendo, existe vedação inclusive constitucional à sua intervenção na esfera privada do sujeito.[25]

---

[24] ALMEIDA, Gilberto Martins de. *Qual a responsabilidade jurídica dos websites*. Módulo e-Security News. mar. 2000. Disponível em: <http://www.modulo.com.br>.
[25] ALMEIDA, Gilberto Martins de. *Qual a responsabilidade jurídica dos websites*. Módulo e-Security News. mar. 2000. Disponível em: <http://www.modulo.com.br>.

Outro norte toma a discussão quando o provedor *edita* o dito conteúdo. Neste caso, há responsabilidade direta pela informação veiculada ou produzida. Analogamente, pode-se dizer que, ao tomar conhecimento de transmissão ou divulgação de informação manifestamente indevida ou imprópria, o provedor torna-se solidariamente responsável, devendo adotar as providências técnicas cabíveis para fazer cessar a irregularidade.[26]

Havendo a presença do consumidor em um dos pólos da relação jurídica, desaparece, por comando legal do Código Brasileiro de Defesa do Consumidor, a necessidade de caracterização da culpa, surgindo a chamada *responsabilidade objetiva ou sem culpa*.

A segurança da continuidade de acesso, por exemplo, assemelha-se ao serviço prestado pela concessionária de serviços públicos, sendo o provedor responsável pela estrutura externa e o consumidor pela interna. Aplicável a *teoria do risco*, através da qual o provedor, razoavelmente observado o estágio de desenvolvimento da tecnologia disponível, assume o risco de sua atividade econômica, obrigando-se a ressarcir o eventual prejuízo direto daí advindo, bem como a reparar o dano decorrente.[27]

As demais empresas que operam na Internet também estão sujeitas a estabelecer relações de consumo, no que devem obedecer às mesmas regras. *Os procedimentos utilizados no comércio pela Internet são exatamente os mesmos verificados no comércio tradicional, verificando-se tão somente alteração na forma e nos mecanismos de contratação, através do desenvolvimento de novas tecnologias.*[28]

Uma última observação cabe a respeito da diferenciação entre os danos oriundos das falhas de segurança em sistemas de informação desenvolvidos sob medida e em aplicativos denominados *de prateleira*, de consumo de massa. Há que se observar que, enquanto estes estão diretamente relacionados ao consumidor final, aqueles podem ser caracterizados como insumos de produção, vez que sua destinação final, não raro, é a utilização comercial, empresarial do software. Daí decorre que o tratamento e as soluções legais devem ser diferenciadas, valendo, em regra, as normas de defesa do

---

[26] Ibid.
[27] PAESANI, Lilian Minardi. *Direito e Internet*; Liberdade de Informação, Privacidade e Responsabilidade Civil. Atlas. São Paulo. 2000. p. 87.
[28] SCHOUERI, Luís Eduardo. *Internet.* O Direito na Era Virtual. 2ª edição. Forense. Rio de Janeiro. 2001. p. 101.

consumidor para o software de massa e as eventuais cláusulas contratuais para produtos *on demand*.[29]

Métodos de Controle de Segurança

Para minimizar as possibilidades de prejuízo representadas pelas ameaças à segurança da informação já expostas, deve-se dispor de mecanismos de controle e de gerenciamento de acessibilidade, tanto de acordo com a relevância da informação que se procura proteger, quanto de acordo, como já foi exposto, com o direito que cada cidadão tem à privacidade e à intimidade.

Para isso, diversos podem ser os métodos que constituem-se em poderosos aliados no combate ao uso desautorizado da informação. Seguem algumas considerações sobre aqueles de utilização mais extensiva no atual estágio de desenvolvimento tecnológico.

Meios Eletrônicos de Identificação

Hoje em dia, não resta dúvida de que o procedimento de autenticação mais barato e mais simples é a atribuição de senhas aos usuários de um sistema ou base de dados. No entanto, a experiência tem demonstrado, que o gerenciamento desta solução nem sempre é tão simples e que os resultados, assim sendo, nem sempre são os esperados. É importante ressaltar que os usuários são, sim, responsáveis pelas suas senhas, assim como os administradores de sistemas são obrigados a garantir o gerenciamento e a proteção das mesmas. Nenhuma técnica ou providência de detecção de ataque será eficiente se o agressor conseguir efetuar o *login* por meio de uma senha válida.[30]

A política de gerenciamento de senhas deve ser muito bem definida e os funcionários devidamente conscientizados e instruídos, de forma a entenderem a responsabilidade que se lhes imputa. Princípios como a troca periódica obrigatória, a impossibilidade de atribuição de seqüências óbvias, datas de nascimento, iniciais dos nomes, podem

---

[29] LONGDIN, Louise. *Liability for Defects in Bespoke Software: Are Lawyers and Informat ion Scientists Speaking the same Language?*. Journal of Law Information Technology, London, v. 8. n.1. 2001. Disponível em: <http://www.jilt.co.uk>.

[30] PEREIRA, Cristiane Santos. Implementação de Políticas e Procedimentos de Segurança em Ambientes Internet. Universidade de Brasília. 2000. p. 54.

parecer elementares, mas importariam em grande redução no potencial de ameaça à segurança de um sistema ou banco de dados.

Hodiernamente, métodos biométricos de identificação (impressão digital, voz, retina) já vêm sendo utilizados, notadamente para indivíduos de funções estratégicas, com acesso a níveis de informação particularmente essenciais e confidenciais, como executivos de grandes instituições financeiras, organizações militares, setores de alta tecnologia, dentre outros.

Importando em custo obviamente maior, essas formas de autenticação de usuários oferecem risco bem menor de acesso indevido. Da mesma forma, é desnecessário lembrar que a responsabilidade pela manutenção e uso da senha de identificação e autenticação é inescusável e intransferível.

Seja qual for o meio de identificação utilizado, praticamente todos os bancos de dados e sistemas operacionais multiusuário disponíveis no mercado disponibilizam para o administrador a opção de manter um arquivo de *log*, a partir do qual é possível identificar acessos, tentados ou consumados, válidos ou forçados, de forma a exercer, então, o devido controle ostensivo.[31]

Assinatura Digital

As assinaturas e os certificados digitais, pela confiabilidade que conferem às transações, e pela já larga utilização comercial e empresarial que alcançaram, tendem a assumir a condição de padrão mundial de autenticação de documentos e operações eletrônicas.[32]

É o que ocorre hoje, por exemplo no Brasil, nos Estados Unidos e na União Européia, onde já existem infra-estruturas legais para a utilização de sistemas baseados na criptografia assimétrica, que embasa a idéia do par de chaves pública/privada.

---

[31] PEREIRA, Raphael. *Como os registros de log podem ajudar nos processo de investigação?* Módulo e-Security Magazine. set. 2001. Disponível em: <http://www.modulo.com.br>.
[32] NETWORK ASSOCIATES INC. *An Introduction to Cryptography.* EUA.1999. p. 13.

Alguma resistência ainda remanesce no meio jurídico nacional quanto à aceitabilidade do documento eletrônico, ainda que revestido das garantias que a tecnologia disponível nos oferece para assegurar-lhe a autenticidade.

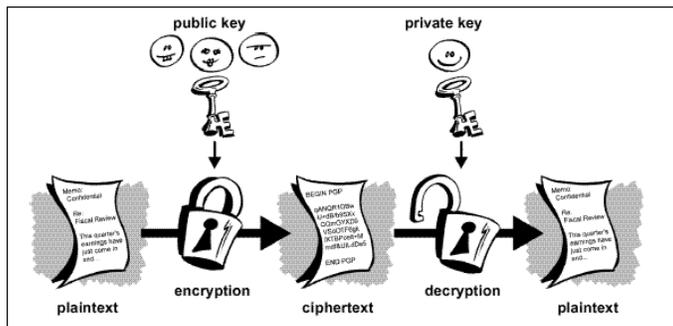



Fig. 06 – Procedimento de codificação e de decodificação de chave pública.
Fonte: An Introduction to Cryptography. Network Associates Inc. 1999.

O problema já foi enfrentado, com competência, pelo Professor Ivo Teixeira Gico Júnior, ao assinalar que a desconfiança parece muito mais um uma restrição de fôro íntimo dos doutrinadores e operadores do direito, do que um problema, um empecilho de fato.

> *Não existe nada mais material ou real que um arquivo eletrônico. Mesmo quando existe apenas na memória RAM (*Random Access Memory*) o documento ainda assim é uma coisa, o resultado de um processo físico-químico que, em uma operação lógica, traduzindo uma infinidade de zeros e uns, a linguagem binária, resulta no documento eletrônico. Não é a dependência do computador para existir que torna o documento eletrônico menos documento.*[33]

A discussão atual concernente à assinatura digital no Brasil, a respeito de quais seriam os órgãos ou as instituições que deveriam possuir autorização e legitimidade para atestar a validade de certificados digitais é pertinente, uma vez que do reconhecimento público da respeitabilidade das autoridades certificadoras e reconhecedoras depende a segurança jurídica e a confiabilidade de todo o sistema nacional de chaves públicas.

---

[33] TEIXEIRA, Ivo Gico Júnior. *O Arquivo Eletrônico como Meio de Prova.* Revista IOB. Rio de Janeiro. 2000. Vol III. 2000. Item 17052.

Controle de Conteúdo

Uma outra forma de estabelecer controle sobre o acesso a informação é por intermédio dos softwares supervisores de conteúdo, que, por intermédio de palavras-chave e de relatórios-padrão de acompanhamento, impedem ou restringem o acesso a determinado tipo de informação, condições previamente estipuladas pelos administradores de sistemas ou pelo *security officer*.

É fácil perceber que a navegação na Internet se transformou em uma gargalo à produtividade. Preocupadas com este panorama, as empresas, paulatinamente restringem sua política de acesso à Internet por meio de configurações especiais de *firewall*, *proxy* ou, ainda, pela monitoração dos *logs*. E começam a punir o que consideram excessos. Na Xerox, por exemplo, quarenta funcionários foram demitidos no ano passado, em várias unidades espalhadas pelo mundo, por uso impróprio da Internet, em *leading cases* mundiais de demissão por justa causa.[34]

Monitoramento de e-mail

O e-mail, de há muito, já se transformou indispensável no mundo dos negócios. Por ser impossível e impensável às empresas visualizar o ambiente de trabalho sem esta ferramenta, elas buscam formas de se proteger do que consideram abusos. Uma delas é monitorar as mensagens eletrônicas, valendo-se de meios de controle de conteúdo. Mais uma vez, a dialética segurança *versus* privacidade vem à tona.

Pesquisa realizada pela revista Info Exame mostra que 34,5% das empresas já monitoram o tráfego das mensagens e 25% pretendem fazê-lo ainda este ano. Responderam à pesquisa, empresas como a Embraer, Pão de Açúcar, Basf, Antarctica, Banco do Brasil, BCP e Usiminas. Uma espiada nas estatísticas do instituto de pesquisas americano Worldtalk Corp*. dá uma idéia do tamanho do problema. Baseado nos dados de 100 empresas, o levantamento mostra que 31% das mensagens corporativas têm conteúdo inadequado (de paquera e correntes a informações sigilosas); 10% são* spam*; 9% contêm arquivos pesados, que congestionam a rede; e*

8% carregam vírus, pornografia ou piadas. "No Brasil, mais de 50% das mensagens que trafegam todos os dias nas redes corporativas são lixo", afirma Mauricio Strasburg, diretor da GS Sistemas, empresa especializada em segurança.[35]

Claro está que o funcionário não pode simplesmente ser devassado porque a empresa acredita que assim estará assegurando a integridade de suas informações confidenciais. No mesmo diapasão, o uso indevido de informação e de recursos computacionais da empresa deve ser, na medida do razoável, evitado, e, se preciso, coibido.

Uma solução coerente seria obter, já no momento da admissão do novo funcionário, *a assinatura do mesmo no documento individual de adesão à política de uso de redes de dados*, *o que pode vir no bojo de outras regras, como diretrizes de ética corporativa e acordo sobre propriedade de obras e invenções*. Os funcionários que já estiverem no curso de seu contrato de trabalho também devem ser comunicados e conscientizados de tais políticas, e, ao final, devem aderir formalmente, por meio de assinatura de termo próprio.[36]

Ainda segundo o autor acima citado, as razões da empresa para a adoção da política em questão, bem como as possíveis repercussões (sanções civis, trabalhistas e criminais) decorrentes de condutas e que forem identificadas através da monitoração também devem ser expressamente divulgadas.

Legislação e Normas

As iniciativas legais de disciplinar o tratamento e a segurança da informação já passam a fazer parte do ordenamento jurídico dos estados e das organizações internacionais.

O Parlamento Sueco, em 1973, foi o responsável pela elaboração do *Datalagen*, a primeira Lei orgânica da Europa visando à proteção da privacidade e dos bancos de dados, tanto públicos quanto privados.

---

[34] MILITELLO, Kátia. *Os perigos da Internet*. Infoexame. São Paulo. 2001. Disponível em: <http://www.infoexame.com.br>.
[35] TERZIAN, Françoise. *EUA vão perder US$ 10 bilhões Sistemas. B2B serão os mais afetados*. TCInet, 2001. Disponível em: <http://www.tcinet.com.br>.
[36] ALMEIDA, Gilberto Martins de. *As Empresas podem "grampear" o e-mail de seus funcionários?* Módulo e-Security News. Rio de Janeiro. 1999. Disponível em: <http://www.modulo.com.br>.

Hoje, segundo boletim informativo do escritório de advocacia americano *McBride, Baker & Coles*, que acompanha a evolução da legislação relativa à Tecnologia da Informação, à privacidade e ao Comércio Eletrônico por todo o mundo, a Comunidade Européia (CE), estipulou cláusulas contratuais de proteção à informação e aos dados pessoais de forma a atender à Diretiva aprovada pela própria CE, que exige *proteção adequada* para qualquer transferência de informação privada para países não-membros. Seguindo tal determinação, os Estados integrantes da União são obrigados a reconhecer os países ou organizações internacionais que respeitem tais cláusulas como sendo instituições que oferecem a assim referida *proteção adequada*.[37]

Ainda na Europa, a Alemanha destacou-se desde muito cedo, demonstrando grande agilidade na elaboração de diplomas legais que buscassem a defesa jurídica dos interesses envolvidos com a segurança da informação. Como exemplo, há legislação alemã, inclusive em matéria penal, responsabilizando provedores inclusive pelo conteúdo dos *links* incluídos nos limites de suas páginas. Em vigor desde 1997, o *Germany Information and Communication Services Act* é uma iniciativa legal de estabelecer padrões e políticas econômicas uniformes e seguras para a transmissão de informação e dados eletrônicos.

Na América Latina, a Colômbia, segundo o mesmo boletim, já elaborou texto legal definindo a assinatura digital, bem como regulamentando a atuação das autoridades certificadoras. A segurança jurídica do certificado digital, à luz da lei colombiana, dependerá da exclusividade pessoal do seu uso, da capacidade de verificação, do controle individual, da invariabilidade técnica, de modo que uma alteração impeça a verificação, e da obediência às formalidade normativas do governo colombiano, requisitos que, uma vez atendidos, conferem ao documento eficácia legal.

No Brasil, o projeto de lei PLS 672/99, cuja redação final segue à Câmara dos Deputados, pretende disciplinar o reconhecimento legal do documento eletrônico, bem como as relações jurídicas relativas ao *e-commerce* e ao intercâmbio eletrônico de dados (IED). Entrementes, as situações jurídicas de fato, que não esperam pela produção

---

[37] MCBRIDE, BAKER & COLES. E-Commerce Spotlight. Summary of E-Commerce Legislation. Disponível em <http://www.mbc.com>.

legislativa, vão sendo resolvidas e conciliadas com base na analogia, no que assim couber.

A respeito, especificamente, da infra-estrutura para chaves públicas – assinatura digital com base em criptografia assimétrica –, o decreto n.º 3.587, de 5 de setembro de 2000, já a define, com respeito ao Governo Federal, complementado pelo decreto n.º 3.865, que estabelece requisitos necessários para a contratação destes serviços pelos órgãos públicos federais.

Alegando as evidentes relevância e urgência da matéria, na Medida Provisória n.º 2.200, reeditada pela segunda vez em 24 de agosto de 2001, o Governo Federal responde à clara pressão do setor privado para a regulamentação de matéria cuja velocidade de desenvolvimento e intenso ritmo de transformação urgem medidas céleres.

A referida MP, portanto, define, em caráter provisório, a infra-estrutura genérica de chaves públicas brasileira, atribuindo competências para a regulamentação, expedição, distribuição e validação de certificados, bem como definindo os requisitos para que a assinatura digital produza efeitos em todas as esferas jurídicas.

Diversas discussões hão de surgir a respeito dos efeitos jurídicos e da adequação das normas propostas à realidade, sendo absolutamente natural o aprimoramento e a atualização periódica dos comandos legais promulgados, instrumentos sem os quais a proteção à esfera de privacidade e à segurança dos dados e da informação corporativa será tarefa inglória e improdutiva.

Considerações Finais

A discussão relativa ao confronto entre o direito à privacidade e o interesse público, entre a preservação da intimidade e o direito coletivo à segurança jurídica da informação, está longe de chegar a termo. Ao contrário, pelos indicadores disponíveis, este será um tema recorrente daqui por diante, à medida em que os sistemas de informação forem se tornando parte ainda mais presente, indissociável e indispensável na vida das pessoas.

Esta nova fronteira da era digital, já atingida pelo escopo de atuação do direito, viverá sempre a reclamar constante atenção e periódica reavaliação, de modo que a tecnologia e os métodos não venham a estabelecer um descompasso social, desarmonizando-se com relação aos princípios e aos valores que devem resguardar.

Há, com efeito, pairando no ar, um sem-número de ameaças à esfera de privacidade do indivíduo, ao intercâmbio eletrônico seguro e confiável de dados, e, por conseguinte, ao desenvolvimento eficiente das relações comerciais e empresariais.

As questões que tratam de segurança e da proteção jurídica da informação corporativa vêm introduzir alterações profundas, significativas, cruciais que, em sede jurídica, tendem a ocorrer inclusive na órbita processual. São procedimentos que irão impactar na maneira como o próprio processo é conduzido. Frise-se, portanto, que não é conveniente que o controle destes atos não esteja ao alcance da compreensão clara de quem, por lei, deve conduzi-los.

É necessário notar, que a esmagadora maioria dos especialistas em atividade no país é de brilhantes e geniais profissionais, que, a despeito da falta de bibliografia disponível, da carência de encontros que propiciem um maior intercâmbio profissional, da ausência de debates públicos e mais criteriosos a respeito dos grandes temas da área, estudam, especializam-se, produzem, resolvem problemas e são muito, muito bons no que fazem.

Autodidatas, no entanto, apesar do inegável romantismo que suas histórias trazem, serão, dentro em pouco, exceções à regra. É preciso deixar de lado o corporativismo que, com freqüência, dispara ondas de protecionismo profissional para entender a

dimensão que o movimento toma. De posse desse entendimento, será patente a necessidade de formar pessoal especializado, tanto para a solução prática e técnica dos problemas e limites que surjam, quanto para a teorização e a análise lógica e jurídica dos litígios que nascerem à sombra deste novo paradigma de mundo.

Quanto aos procedimentos e técnicas aqui expostos, apresentam, inegavelmente, limitações à solução satisfatória do problema da segurança apresentado. Limitações técnicas, contudo, são superáveis. As máquinas ficam mais rápidas, o tempo de processamento diminui, a capacidade de armazenamento aumenta. É por isso que, no momento, parece ser muito mais relevante discutir o *fundamento*, o *objeto* ou *interesse jurídico* que pretendemos proteger ao tratar da necessidade de segurança da informação corporativa, *de quem* queremos protegê-la, *para que, a que custo* social e econômico e *até que ponto*, decisões – essas sim – perenes, e que determinarão políticas e rumos.

Curioso é notar, conforme lembra PAESANI (2001), que não há governos autoritários ou regimes totalitaristas fundamentando as ameaças a que o trabalho se refere. Elas decorrem do próprio progresso, que, por sua vez, somente foi permitido pela liberdade de criação e de pensamento e do incentivo à livre iniciativa, características típicas dos regimes democráticos, liberais.

Isto tomado no âmbito das relações internacionais, e posto que nem todas as nações terão a oportunidade de debate com a mesma profundidade, ou acesso, em igualdade de condições, aos mecanismos e às tecnologias de controle, é fácil constatar que este domínio da segurança da informação fatalmente há de se constituir em instrumento de imensa vantagem política e econômica, cabendo certamente ao direito, papel fundamental no sentido de disciplinar e estabelecer limites a esta desmedida vantagem, de impedir desequilíbrios flagrantes e injustos e de dar contornos menos sombrios ao lema que acompanha a sociedade da informação, desde o seu nascedouro.

Who controls the past,
controls the future.
Who controls the present,
controls the past.

George Orwell, 1984.

Bibliografia

ABREU, Dimitri. *Melhores Práticas para Classificar as Informações*. Módulo e-Security Magazine. São Paulo. ago. 2001.

ALMEIDA, Gilberto Martins de. *As Empresas podem "grampear" o e-mail de seus funcionários?* Módulo e-Security News. Rio de Janeiro. 1999.

ALMEIDA, Gilberto Martins de. *Qual a responsabilidade jurídica dos websites*. Módulo e-Security News. mar. 2000.

BAKER & MCKENZIE. Escritório de advocacia europeu especializado em Direito de Tecnologia da Informação Propriedade Intelectual e Comércio Eletrônico. <http://www.bakermckenzie.com>.

BITTAR, Carlos Alberto, BITTAR, Carlos Alberto Filho. *Tutela dos Direitos da personalidade e dos Direito Autorais nas Atividades Empresariais*; São Paulo: Revista dos Tribunais; 1993.

BRASIL EM TEMPO REAL. *Senado Aprova Normas de Acesso à Internet*. Brasília. ago. 2001. Disponível em: <http://emtemporeal.com.br>.

BORAN, Sean. *The IT Security Cookbook Information classification.* EUA. dez. 1996.

BORKING, John J. RABB; Charles D. *Laws PETs and Other Technologies for Privacy Protection.* Journal of Law Information Technology. London, *v*.8, n.1, fev. de 2001.

BOTONI, Fernanda. *Sos Backup.* Infoexame, Rio de Janeiro. set. 2001.

CAMPOS, Eduardo. *Investimentos em Segurança da Informação. Como Justificar?* Jornal da Segurança. São Paulo. mar. 1998.

CÓDIGO CIVIL. 14ª edição. Saraiva. São Paulo. 1999.

CÓDIGO DE DEFESA DO CONSUMIDOR COMENTADO PELOS AUTORES DO ANTEPROJETO. 4ª Edição. Forense Universitária. São Paulo. 1995.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL.. 20ª edição. Saraiva. São Paulo. 1998.

COSTA, José Carlos Netto. *Direito Autoral no Brasil.* FTD. São Paulo. 1998.

COVALLA, Tom. Safe and Sound. *Management Directions*. EUA, set. 2001. n.21. p. 5.

GUEIROS, Nehemias Júnior. *Direito Autoral No Show Business*. A Música. 2ª edição. Gryphus. Rio de Janeiro. 2000.

IDC – Empresa de análise mercadológica e estratégica em Tecnologia da Informação. Disponível em: <http://www.idc.com>.

INFOEXAME. Portal da Revista Infoexame <http://www.infoexame.com.br>

INFORMATION WEEK, *PriceWaterhouseCoopers & Global Information Security Survey.* Information Week. EUA, 2001.

INTERNET SECURITY SYSTEMS. *Recognizing the Need for Enterprise Security Management – An Introduction to SAFEsuite® Decisions*. EUA. 2000.

LESSIG, Lawrence. *The Architecture of Privacy. Conferência na Taiwan Net*. Taipei. mar. 1998.

LOBO, Paulo. *Direito e Globalização*. FACTUM, Informativo Jurídico. Campina Grande, set.1998. p.02

LONGDIN, Louise. *Liability for Defects in Bespoke Software: Are Lawyers and Information Scientists Speaking the same Language?.* Journal of Law Information Technology, London, v. 8. n.1. 2001.

MARTINS, Fran. *Curso de Direito Comercial.* Forense. Rio de Janeiro. 1999.

MCBRIDE, BAKER & COLES. Escritório de advocacia americano especializado em Direito de Tecnologia da Informação e Comércio Eletrônico. EUA. <http://www.mbc.com>.

MILITELLO, Kátia. *Os perigos da Internet*. Infoexame, São Paulo, 2001. Disponível em: <http://www.infoexame.com.br>

MÓDULO SECURITY SYSTEMS. Empresa especializada em Segurança da Informação. Editora do Informativo *e-Security News* e da Revista Eletrônica *e-Security Magazine*. <http://www.modulo.com.br>.

NETWORK ASSOCIATES INC. *An Introduction to Cryptography.*EUA.1999.

PAESANI, Lilian Minardi. *Direito e Internet*; Liberdade de Informação, Privacidade e Responsabilidade Civil. Atlas. São Paulo. 2000.

PERDONCINI, Priscila. *Arquivos Públicos na Internet Ameaçam Privacidade*. InfoGuerra. ago. 2001. Disponível em: <http://www.infoguerra.com.br>.

PEREIRA, Cristiane Santos. *Implementação de Políticas e Procedimentos de Segurança em Ambientes Internet*. Universidade de Brasília. 2000.

PEREIRA, Raphael. *Como os registros de log podem ajudar nos processo de investigação?* Módulo e-Security Magazine. set. 2001.

REVISTA DA CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. *Com um pé no Futuro*. Brasília n.311. fev. 1999.

SCHLARMAN, Steven; *Enterprise Security Architecture System*. PriceWaterhousCoopers. jul. 2000.

SCHOUERI, Luís Eduardo. *Internet.* O Direito na Era Virtual. 2ª edição. Forense. Rio de Janeiro. 2001.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 15.edição. Malheiros Editora. São Paulo. 1998.

SOARES, José Carlos Tinoco. *Lei de Patentes, Marcas e Direitos Conexos*. Revista dos Tribunais. São Paulo. 1997.

STOCCO, Rui; FIGUEIRA, Joel Dias Júnior. *Responsabilidade Civil do Fabricante e Intermediários por Defeitos de Equipamentos e Programas de Informática*. Revista dos Tribunais. São Paulo. 2000.

STOCCO, Rui. *Responsabilidade Civil e sua Interpretação Jurisprudencial*. Revista dos Tribunais. São Paulo. 2000.

TERZIAN, Françoise. *EUA vão perder US$ 10 bilhões Sistemas. B2B serão os mais afetados*, TCInet, 2001. Disponível em: <http://www.tcinet.com.br>

TCINET. Portal de serviços e notícias referentes à Tecnologia da Informação <http://www.tcinet.com.br>.

TEIXEIRA, Ivo Gico Júnior. *O Arquivo Eletrônico como Meio de Prova.* Revista IOB. Rio de Janeiro. 2000.

TIMMONS, Cindi, TIMMONS, Aaron. *The Right to Be Left Alone: An Examination of the Right of Privacy*. Greenhill SchoolDallas, Texas. 1998. Disponível em: <http://www.nfhs.org/>

TOLEDO, Antonio Luiz de, Siqueira, Luiz Eduardo Alves et al. *Consolidação das Leis do Trabalho*. 27 edição. Saraiva. São Paulo. 2000.

VENOSA, Sílvio de Salvo. *Direito Civil*. Direitos Reais. Editora Atlas S.A. São Paulo. 2001. v.04.

ZAKABI, Rosana. *HACKERS - Os nossos sãos campeões*. Revista VEJA. São Paulo. set. de 2001.